Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Thiago Braga de Sá Mello

AUTENTICAÇÃO FORTE EM ACESSOS REMOTOS: Análise comparativa entre soluções com três fatores de autenticação e estudo de caso sobre o B-Unit

Rio de Janeiro

2008

Thiago Braga de Sá Mello

AUTENTICAÇÃO FORTE EM ACESSOS REMOTOS: Análise comparativa entre soluções com três fatores de autenticação e estudo de caso sobre o B-Unit

Monografia apresentada para obtenção de título de Especialista em Gerencia de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Rede de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Prof. Mônica Ferreira da Silva, D.Sc., UFRJ, Brasil

Rio de Janeiro

2008

Thiago Braga de Sá Mello

AUTENTICAÇÃO FORTE EM ACESSOS REMOTOS: Análise comparativa entre soluções com três fatores de autenticação e estudo de caso sobre o B-Unit

Monografia apresentada para obtenção de título de Especialista em Gerencia de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Rede de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em dezembro de 2008.

Prof. Mônica Ferreira da Silva, D.Sc., UFRJ, Brasil

RESUMO

MELLO, Thiago Braga de Sá. **AUTENTICAÇÃO FORTE EM ACESSOS REMOTOS: Análise comparativa entre soluções com três fatores de autenticação e estudo de caso sobre o B-Unit**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2008.

Este trabalho tem como objetivo estudar soluções de autenticação forte, utilizando três fatores de autenticação, para acesso remoto corporativo. Neste texto não só abordamos o funcionamento técnico das soluções, mas também aspectos de negócio, através de um estudo de caso sobre uma das soluções verificadas, o B-Unit da Bloomberg. A autenticação forte é uma realidade para o segmento corporativo, sendo bastante utilizada nos casos de acesso remoto. O modelo de dois fatores de autenticação ainda é o mais utilizado, contudo, acreditamos que sua utilização em ambientes hostis demande mecanismos mais confiáveis, que maximizam a garantia de autenticidade do usuário remoto, abrindo mercado para as soluções de três fatores de autenticação.

ABSTRACT

MELLO, Thiago Braga de Sá. **AUTENTICAÇÃO FORTE EM ACESSOS REMOTOS: Análise comparativa entre soluções com três fatores de autenticação e estudo de caso sobre o B-Unit**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2008.

This paper aims to explore solutions for Strong Authentication, using three-factors authentication to corporate remote access. This paper does not focus only in the solutions technical operation, but also in aspects of business through a case study: the B-Unit Bloomberg. The strong authentication is a reality for corporations and is often used for remote accesses. The two-factor authentication model is still the most widely used, however hostile environments may demand more reliable mechanisms maximizing the guarantee of authenticity for the remote user, opening market for the solutions of three factors-authentication.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

FIPS	Federal Information Processing Standards
LCD	Liquid Crystal Display
OTP	On-time password
PDA	Personal Digital Assistant
PIN	Personal Identification Number
RFID	Radio Frequency Identification

SUMÁRIO

1 **INTRODUÇÃO**

1.1 MOTIVAÇÃO

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, conseqüentemente, necessita ser adequadamente protegida. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio (ABNT, 2001).

Sendo assim, proteger a informação é obrigação de toda organização, independente do seu tamanho, concluindo que a proteção do acesso a informação não é uma questão puramente técnica, ela é, principalmente, uma questão de negócio da organização.

Com a demanda crescente de acesso remoto corporativo, torna-se cada vez mais premente que as organizações invistam em processos e tecnologias, se estruturando para mitigar fraudes de identificação eletrônica.

1.2 OBJETIVO

Esta monografia tem por objetivo comparar soluções de autenticação forte que maximizam a garantia de identificação de um usuário remoto e realizar um estudo de caso sobre uma dessas soluções, o B-Unit.

2 **REFERENCIAL TEÓRICO**

2.1 CARACTERIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

Segundo a ABNT (2001), podemos caracterizar a Segurança da Informação pela preservação dos seguintes itens:

a) Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
b) Integridade: salvaguarda da exatidão e completeza da informação e métodos de processamento;
c) Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Para autenticação forte em acessos remotos, estamos preocupados em garantir a confidencialidade da informação através de métodos de autenticação mais robustos.

2.2 CONTROLE DE ACESSO – IDENTIFICAÇÃO X AUTENTICAÇÃO

Com o intuito de oferecer segurança, o acesso aos recursos das organizações depende de um processo de verificação dos usuários. Somente o usuário legítimo deve ter acesso a esses recursos. Esse processo é chamado autenticação.

A autenticação tem um papel fundamental para a segurança de um ambiente corporativo. Sua função é validar a identificação dos usuários.

A identificação é a função em que o usuário declara uma determinada identidade ao sistema, e a autenticação é a função responsável pela validação da identidade declarada.

A segurança do processo de validação depende de uma série de considerações:

a) A forma da coleta dos dados de autenticação;
b) O método de transmissão desses dados;
c) E a garantia de que o usuário, já cadastrado, é o verdadeiro.

Para autenticação forte em acesso remoto, estamos preocupados em garantir que o usuário que está acessando, e já cadastrado, seja o verdadeiro, inclusive quanto a sua presença física no processo de autenticação.

2.3 FATORES DE AUTENTICAÇÃO

A validação da identificação do usuário pode ser realizada através de três métodos:

a) Autenticação com base no que o usuário sabe: é fundamentada em algum conhecimento do usuário como senha, frase de segurança ou PIN (*Personal Identification Number*). As senhas são o método mais utilizado, uma vez que usuários e administradores já estão familiarizados com a sua utilização.
b) Autenticação com base no que o usuário possui: é fundamentada em algum dispositivo que pertence ao usuário, sendo eles dispositivos de memória (*memory token*) - que apenas armazenam informações, dispositivos inteligentes (*smart tokens*) - que além de armazenar, processam informações e os dispositivos senha descartável (*one-time password – OTP*) – que geram novas senhas em períodos regulares ou quando são ativados.

c) Autenticação com base nas características do usuário: É um método que analisa as características físicas ou comportamentais de um indivíduo, comparando-as com os dados armazenados no sistema de autenticação (biometria). A biometria é considerada um método bastante seguro, o reconhecimento é feito unicamente por aspectos humanos intrínsecos.

Definimos como autenticação forte o procedimento de autenticação de um usuário que utiliza, simultaneamente, pelo menos dois fatores acima listados.

2.4 AUTENTICAÇÃO COM DOIS FATORES

Atualmente a autenticação com dois fatores é a solução de mercado para a autenticação forte. A autenticação realizada com a combinação de dois fatores tanto pode ser utilizada para acesso local aos recursos tecnológicos das instituições quanto em casos de acesso remoto. Na prática, ela é amplamente utilizada apenas pelos casos de acesso remoto e, para acesso local, apenas para usuários de missão crítica, como diretores e gerentes.

Nos casos de acesso local, tendo como premissa um ambiente controlado por uma solução de autenticação de acesso físico (por exemplo, o crachá), podemos considerar a autenticação de dois fatores como suficiente para garantir a autenticidade da identificação do usuário. Para ambientes hostis, onde não há garantia mínima de quem está tentando realizar o acesso, outras formas de autenticação forte deveriam ser avaliadas.

2.5 AUTENTICAÇÃO COM TRÊS FATORES

A autenticação de três fatores, como o próprio nome já diz, é o método de autenticação que agrupa um fator de autenticação de cada um dos três grupos de

fatores de autenticação. A utilização de quatro ou mais fatores de autenticação só tornaria o método de autenticação redundante quanto ao fator, não agregando maior nível de segurança ao processo de autenticação.

O processo de autenticação por três fatores é especialmente útil quando lidamos com ambientes hostis, uma vez que ele maximiza a garantia de autenticidade do usuário remoto, utilizando os três grupos de fatores de autenticação para obter maior acuracidade no processo. Os usuários remotos são testados ao máximo da tecnologia, quanto ao que eles sabem, ao que possuem e a quem eles são.

2.6 A BLOOMBERG E O RECURSO DE BLOOMBERG ANYWHERE

A Bloomberg é um dos principais provedores mundiais de informação para o mercado financeiro. Os terminais de informações Bloomberg (Figura 1) estão presentes em quase 100% dos bancos, corretoras e seguradoras no mundo. Possuem também uma emissora de TV a cabo – a Bloomberg Television – que faz a transmissão ao vivo das principais bolsas de valores ao redor do mundo, bem como entrevistas e matérias sobre o mercado financeiro. A Bloomberg publica também livros e revistas com conteúdo financeiro e relatórios diversos.

Figura 1 - Terminal Bloomberg

O investimento mensal em um terminal Bloomberg é da ordem de US$1.500,00 por mês, sem contabilizar os links necessários. Basicamente existem dois tipos de terminal, o de consulta – com um usuário e senha compartilhados por todos da empresa, e que possui apenas as funções de leitura de informações, e o terminal de operação – necessariamente atrelado a um único usuário e com solução de autenticação de dois fatores, senha e biometria.

Todo terminal Bloomberg de operação licencia o usuário a também utilizar o recurso de Bloomberg Anywhere, que é a solução de acesso remoto ao sistema da Bloomberg, onde um processo de autenticação de três fatores é utilizado.

Após o processo de autenticação, o usuário é capaz de trabalhar remotamente como se estivesse dentro da empresa.

2.7 O B-UNIT

O B-Unit (Figura 2) é uma solução proprietária da Bloomberg que permite a autenticação de um usuário remoto. Os fatores utilizados são:

a) Autenticação com base no que o usuário sabe: senha
b) Autenticação com base no que o usuário possui: o próprio B-Unit
c) Autenticação com base nas características do usuário: biometria

Figura 2 - Bloomberg B-Unit

As características do equipamento podem ser visualizadas pela Figura 3.

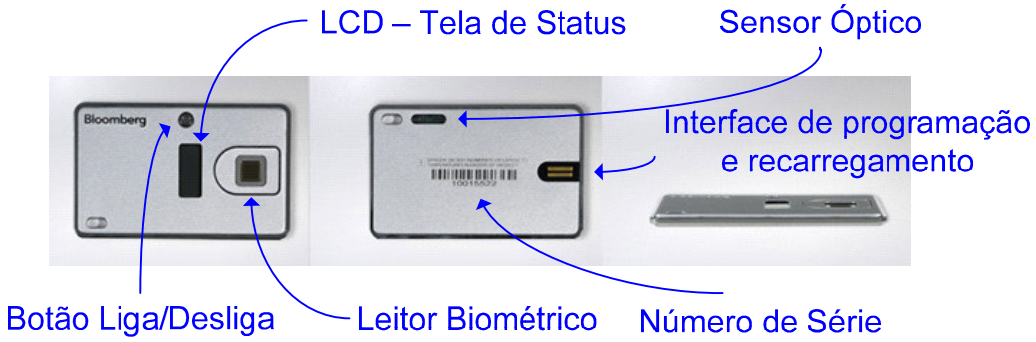

Figura 3 - Bloomberg B-Unit - Características

O B-Unit foi arquitetado para uso pessoal e intransferível. Quando entregue ao usuário, o primeiro procedimento é o cadastro de sua digital através de um processo de amostragem, sendo possível cadastrar no equipamento uma única digital (BLOOMBERG, 2004). Ao fim do processo, o B-Unit fica associado ao usuário e atrelado aos sistemas da Bloomberg através de seu número de série único (Figura 3).

Os três fatores de autenticação são conjugados da seguinte forma:

1. Através de um *browser*, o usuário acessa o site do sistema Bloomberg Anywhere e inicia o processo de autenticação inserindo o nome do seu usuário e sua senha (o que o usuário sabe). Uma nova página é aberta com uma figura de formato retangular e cor vermelha piscando;
2. Em seguida, o usuário deve pressionar uma vez o botão de ligar do B-Unit e aguardar a mensagem "*present finger*" ser apresentada no visor de LCD do equipamento. Nesse momento o usuário deve posicionar sua digital (o que o usuário é), previamente cadastrada, no sensor óptico do B-Unit. Uma vez que a digital é reconhecida, a mensagem de "Ready to Sync" é apresentada no LCD do B-Unit;

3. Na etapa final do procedimento o usuário deve ter o B-Unit no local onde o acesso remoto está sendo feito (o que o usuário possui), posicionando o sensor óptico do mesmo a cerca de três centímetros da figura de formato retangular e cor vermelha vibrante que está aparecendo no monitor. O B-Unit é capaz de ler o código vibrante que está sendo transmitido pelo monitor e, juntamente da validação biométrica já realizada, o mesmo gera em seu LCD uma contra-senha de quatro caracteres alfanuméricos. Para finalizar esse processo de desafio-resposta, a contra-senha é inserida manualmente pelo usuário no site, finalizando o processo de autenticação e iniciando o acesso ao produto Bloomberg Anywhere.

O B-Unit também pode ser usado como dispositivo de dois fatores de autenticação, ignorando a biometria. Esse processo é especialmente útil para usuários que possuem problema com suas digitais (como é o caso de usuários com pele muito fina), pessoas alérgicas a níquel, ou que possuem problemas epiléticos ou distúrbios psiquiátricos.

2.8 OUTRAS SOLUÇÕES DE TRÊS FATORES DE AUTENTICAÇÃO

2.8.1 **O PlusID da Privaris**

Figura 4 - PlusID da Privaris - Características

O PlusID é uma solução de três fatores de autenticação produzida pela empresa americana Privaris, os fatores utilizados são:

a) Autenticação com base no que o usuário sabe: senha

b) Autenticação com base no que o usuário possui: o próprio PlusID

c) Autenticação com base nas características do usuário: biometria

O equipamento é modular, podendo ser usado tanto com dois ou três fatores (Figura 4). Quando usado com dois fatores, o fator que se baseia no que o usuário sabe não é utilizado.

Ao invés de usar um display LCD para apresentar a contra-senha do desafio-resposta, o PlusID utiliza uma das seguintes tecnologias de transmissão, com e sem fio, para levar o resultado até o equipamento que desejamos acessar: RFID, Bluetooth ou USB.

Essas tecnologias de transmissão tornam o PlusID apto a trabalhar não só com sistemas, mas principalmente a ter interface com outros dispositivos físicos. Podemos citar soluções de controle de acesso físico como exemplo, onde o usuário deve estar com o PlusID no local que deseja ser acessado (o que o usuário possui), passar sua digital no sensor biométrico do PlusID (o que o usuário é), aproximá-lo do sensor de presença da porta (RFID) para em seguida digitar sua senha no teclado da porta (o que o usuário sabe), finalizando o processo de autenticação por três fatores (PRIVARIS, 2007).

2.8.2 **Tri-D 3-Factor Biometric Card da Tri-D**

O Tri-D é uma solução de três fatores de autenticação produzida pela empresa americana de mesmo nome, os fatores utilizados são:

a) Autenticação com base no que o usuário sabe: senha

b) Autenticação com base no que o usuário possui: o próprio Tri-D

c) Autenticação com base nas características do usuário: biometria

O equipamento é modular, podendo ser usado tanto com dois ou três fatores de autenticação (Figura 5).

Figura 5 - Tri-D - Caracteríticas

Quando usado com dois fatores, o fator que se baseia no que o usuário sabe não é utilizado.

A identificação biométrica é o ponto de partida para a utilização do Tri-D, ativando o sistema de transmissão sem fio RFID, a senha descartável (OTP) ou o módulo de *smart-card*. A biometria ativa um desses sistemas, nunca dois deles ao mesmo tempo (TRI-D, 2008).

Como solução de três fatores, ele pode funcionar da mesma forma que a solução da Plus-ID, com a limitação de transmitir a contra-senha apenas por RFID ou ativando o *smart-card*. O LCD não é utilizado nesses casos.

Essa solução é semelhante ao B-Unit quando usamos o visor de LCD ao invés do RFID para transmitir a contra-senha para o equipamento/sistema que desejamos acessar. O ponto de diferença no processo é que neste caso não podemos garantir que o usuário está no local da autenticação, uma vez que nenhum método de sincronismo no local físico do acesso é utilizado. Em verdade, o usuário

pode estar em outro local passando a informação gerada no LCD (OTP) via telefone para um terceiro que estará efetuando o acesso indevido.

2.9 ANÁLISE COMPARATIVA ENTRE AS SOLUÇÕES APRESENTADAS

2.9.1 **Mobilidade**

Quando discutimos soluções de acesso remoto, o primeiro ponto a ser abordado é a mobilidade da solução. O acesso remoto deve ser seguro, usando autenticação forte, mas nem por isso pode ser um processo complicado para o usuário final.

As soluções apresentadas possuem níveis de mobilidade diferentes. O B-Unit foi a única solução de três fatores que não precisou de um leitor externo específico para funcionar, uma vez que ele sincroniza diretamente com o monitor do usuário. Por sua vez, o PlusID sempre irá precisar ou de um leitor de Bluetooth ou RFID ou ainda de uma entrada USB, enquanto o Tri-D, quando utilizado pelo LCD, se iguala em mobilidade ao B-Unit (nos outros modos ele precisará de algum tipo de leitor), mas não consegue garantir que o usuário que está acessando está realmente presente no momento do acesso.

2.9.2 **Serviços Agregados**

As soluções de acesso remoto também devem ser avaliadas quanto à quantidade de serviços distintos que elas podem agregar. Nesses termos, PlusID e Tri-D possuem colocação diferenciada. O destaque está no PlusID, com recursos de RFID e Bluetooth, podendo interagir a distância com os mais distintos equipamentos de TI. Em seguida está o Tri-D, que também possui o recurso de RFID e um *smart-card*. O B-Unit, por ser uma solução proprietária da Bloomberg, somente pode ser utilizado para acesso remoto em seus terminais, não sendo passível de utilização em outros locais da corporação.

2.9.3 **Universalidade de uso**

Levando em consideração o fato de que alguns indivíduos possuem dificuldade em ter suas digitais reconhecidas e outros possuem alergia a níquel, material presente em todos os leitores apresentados, a solução de mobilidade deve prever alguma forma de acesso para esses usuários.

Verificamos que apenas o B-Unit é capaz de apresentar uma forma de acesso diferenciada para esses usuários, mesmo assim diminuindo um fator de autenticação (biometria). As outras soluções partem da premissa de o usuário possuir uma digital para ser detentor do produto, o que nem sempre será verdade.

3 METODOLOGIA DE PESQUISA

A pesquisa realizada foi qualitativa.

O método utilizado foi o de estudo de caso.

Para levantamento de dados, foram feitas entrevistas com um gerente de contas da Bloomberg, um responsável técnico da Bloomberg pelo B-Unit e um usuário final do B-Unit através de roteiro de entrevista conforme Anexo A.

4 DESCRIÇÃO DO CASO B-UNIT

4.1 PERSPECTIVA DO GERENTE DE CONTA

O gerente de contas entrevistado trabalha na Bloomberg há quatro anos, estando pelo mesmo período nesta função. Formou-se em administração pela UFRJ e possui pós-graduação em finanças pelo IBMEC. Anteriormente trabalhou por três anos na Reuters. Ele entende que a segurança da informação é algo imprescindível para o ramo em que a Bloomberg atua porque a empresa se preocupa tanto com as informações que são providas quanto com a segurança de acesso das mesmas. Segundo o gerente de contas, a visão de negócio para o B-unit é ser um produto tecnologicamente diferenciado para os usuários, permitindo o acesso remoto de qualquer lugar ao terminal Bloomberg. O gerente de contas afirmou que o B-unit garante que o usuário final seja ele mesmo não havendo a possibilidade do usuário operar sem o dispositivo. Além disso, o equipamento é uma solução idealizada para o mercado financeiro, substituindo o token OTP como solução de autenticação de usuário remoto.

O B-unit tem uma boa aceitação no mercado de forma que seus usuários não o trocam por outra solução. O gerente de contas afirmou não conhecer nenhum outro provedor de informação para o mercado financeiro que tenha uma solução de autenticação como o B-unit, uma vez que esta é uma solução proprietária. O B-Unit não é comercializado porque a Bloomberg prima por oferecer aos seus usuários soluções inovadoras diferenciadas, como foram os casos dos monitores LCD duais, numa época onde o LCD ainda não era popular, e dos teclados com teclas extras e coloridas, simplificando a utilização do sistema. Ainda segundo o gerente de contas, seria necessário que o B-unit se capacitasse para que todos os dispositivos de

mobilidade, como PDAs, Blackberrys e Iphones, suportassem essa solução de forma a representar realmente o principio “Bloomberg Anywhere” (Bloomberg em qualquer lugar). Para a próxima versão serão apresentados equipamentos coloridos que chegarão ao Brasil a partir de janeiro de 2009.

4.2 PERSPECTIVA DO TÉCNICO

Para representar o perfil técnico foi entrevistado um Analista de Suporte de TI da Bloomberg, onde trabalha há onze anos na mesma função, dado que a Bloomberg possui estrutura extremamente horizontal, permitindo crescimento sem troca de cargo. Entretanto, ele é um gerente informal responsável por outros técnicos e terceiros em um Estado brasileiro. Fez segundo grau técnico em eletrônica na escola Visconde de Mauá, iniciou engenharia de telecomunicações na UERJ. Recentemente concluiu o curso de tecnólogo em Processamento de dados na Universidade Estácio de Sá. Ele já trabalhou por cinco anos na Unisys.

Segundo o analista, a segurança da informação pode ser vista por dois aspectos: autenticação remota forte e necessidade de segurança de borda (equipamentos de rede, como firewall). Dessa forma, a empresa em que trabalha investe pesado em tecnologia, buscando sempre estar na frente das concorrentes. O analista aponta como ponto forte da solução de acesso remoto a possibilidade de se realizar negociações via terminal em qualquer lugar de forma segura, uma vez que o equipamento realiza autenticação forte envolvendo três fatores. Já como ponto fraco, foi citado que os usuários reclamam de ter de levar o B-Unit sempre com eles. Os problemas mais comuns ligados à solução se referem à bateria que deveria durar cerca de cinco anos, no entanto, na prática, dura em média, dois anos, só podendo ser recarregada na própria Bloomberg. Apesar disso, o usuário pode estar em qualquer lugar do mundo e o B-Unit é trocado no caso da bateria acabar ou de furto,

denotando que o serviço é totalmente Anywhere. A implantação do B-Unit é simples, mas alguns casos requerem atenção diferenciada. Por exemplo, a implantação do dispositivo é simples porque o usuário coloca o dedo três vezes no sensor para cadastrar a biometria e, no caso de a impressão digital ser de difícil leitura, existe um método de cadastro que utiliza oito amostragens ao invés de três. Entretanto, a biometria não pode ser utilizada por pessoas com pele muito fina, de forma que o usuário utilizará apenas o modo de token, ou seja, apenas dois fatores de autenticação (sem biometria), como era feito antes da existência do B-Unit.

Em sua opinião, a solução de acesso remoto deveria ser mais flexível e incorporar funções do dia a dia, por exemplo, existiu uma versão do B-Unit com MP3 incorporado que não foi comercializada porque a Bloomberg teria chamados de suporte para problemas com o MP3 player, o que de longe é o foco da empresa. No entanto, ele acredita que inserir um sistema aberto de crachá no B-Unit poderia ser interessante porque, na maioria das instituições onde o B-Unit é instalado, o controle de chegada e saída dos funcionários é feito através do crachá, assim, essa funcionalidade seria uma maneira de fazer o B-Unit ser mais útil para o cliente, substituindo o crachá do mesmo. Como novidade, em Nova Iorque, o B-unit já é oferecido aos usuários em diversas cores, desde preto até o rosa. O analista também citou que o B-Unit não pode ser utilizado em monitores de laptop programados em economia de energia com brilho fraco porque o sensor não sincroniza. Ele também não pode ser utilizado por pessoas que sofram de epilepsia ou distúrbios psiquiátricos, devido à tela vermelha de sincronismo vibrante, por pessoas com pele muito fina e, conseqüentemente, sem digital, e pessoas com alergia a níquel, já que o sensor biométrico utiliza este metal para fazer a leitura da digital (o leitor não é óptico).

4.3 PERSPECTIVA DOS USUÁRIOS FINAIS

O usuário entrevistado trabalha no Banco BBM atuando como operador de Bolsa há três anos. Graduou-se em economia pela PUC-Rio e possui mestrado em economia pela mesma instituição. Trabalhou por dois anos no banco Pactual como analista de *equities*.

Segundo o trader, a segurança da informação é importante para os dados com os quais ele opera, sendo imprescindível o alto comprometimento da empresa em que trabalha com estas questões. O operador recorda que o acesso ao Bloomberg Anywhere antes do B-unit era feito através do token. Em sua opinião, a solução atual, tanto quanto a anterior, são inconvenientes, uma vez que ele é obrigado a levar um equipamento em viagem para conseguir trabalhar remotamente. A adaptação ao B-unit levou menos de dois meses, no entanto, o equipamento é esquecido em casa até hoje. Por esse motivo, apesar do B-unit garantir com mais segurança que outra pessoa não se passe por ele em uma operação financeira, o trader voltaria à solução de token que, como vantagem, por exemplo, cita que ao esquecer-se o token, o acesso poderia ser estabelecido através de uma ligação para sua casa. Ele acredita que outras funções do dia-a-dia dele poderiam ser repassadas para o B-Unit, provavelmente algum serviço da própria instituição onde ele trabalha, no entanto ele não saberia exemplificar. Também segundo o trader, o B-unit não influenciou na escolha da Bloomberg como serviço de informação, a qualidade do serviço de informação por si só já é suficiente para edificar sua escolha.

4.4 ANÁLISE DO CASO

Os entrevistados possuem opiniões semelhantes quanto à segurança agregada pela B-Unit. No entanto, podemos verificar que o usuário final possui maior preocupação com a facilidade de uso do que com a segurança em si, inclusive acreditando que a solução anterior era mais interessante, uma vez que o fato dele esquecer o equipamento em casa não restringia por completo o acesso do mesmo.

Houve unanimidade quanto a agregar outras funções ao equipamento, mesmo o usuário final não sabendo exemplificar o que poderia ser. Nesse ponto, podemos verificar que todos, de alguma forma, são usuários do B-Unit e o ato de transportar um equipamento, mesmo pequeno, de função muito específica, não os agrada.

O gerente de contas focou sua análise no universo de soluções de autenticação forte, onde seu comparativo enfatiza os concorrentes do setor de Sistemas de Informações para o mercado financeiro. O técnico realça o quanto a Bloomberg está sendo pioneira na utilização desse processo de autenticação forte por três fatores.

Independente do cargo ou função e mesmo com definições diferentes para Segurança da Informação, todos entendem a questão como sendo importante.

5 **CONCLUSÕES**

A autenticação forte é uma realidade para o segmento corporativo, sendo a autenticação de dois fatores amplamente utilizada para o acesso remoto. No entanto, através de alguns exemplos, conseguimos verificar que dois fatores por si só não conseguem maximizar a garantia de autenticidade do usuário remoto.

Mesmo em ambientes controlados, principalmente dentro dos segmentos corporativos que requerem segurança diferenciada, a segurança por dois fatores deverá estar presente na estação de trabalho de cada usuário nos próximos anos. Para ambientes hostis, onde o acesso remoto é utilizado, devemos observar o crescimento das soluções de três fatores de autenticação. Mecanismos de autenticação confiáveis são críticos para a segurança de qualquer sistema de informação automatizado (FIPS, 1994).

Acreditamos que, como solução de autenticação forte, o B-Unit consegue atingir seu objetivo, tanto em mobilidade quanto em segurança. No entanto, revendo as informações da análise comparativa com o estudo de caso, é interessante verificar que as outras soluções de autenticação preenchem a lacuna deixada pelo B-Unit quanto à possibilidade de agregar outros serviços. Contudo, este fato não deve ser considerado, uma vez que o objetivo do B-Unit não é ser comercial.

A autenticação forte com três fatores ainda é uma tecnologia nova e os grandes fabricantes de soluções de autenticação com dois fatores, como RSA e Aladdin, ainda não entraram neste mercado. Acreditamos que a evolução dessas soluções deva ser verificada em conjunto das descritas nesse material. Outro ponto que agregaria bastante informação seria a realização de estudos de caso das outras soluções de autenticação de três fatores que foram descritas nesta monografia.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, **NBR 17799: Tecnologia da informação - Código de prática para a gestão da segurança da informação. Rio de Janeiro**, ABNT, 2001.

NAKAMURA, EMÍLIO T. E GEUS, PAULO LÍCIO DE, **Segurança de Redes em ambientes cooperativos 2a. ed**., Editora Futura/Siciliano, São Paulo, 2003.
SOARES, L.F.G. et al, **Redes de Computadores: das LANs, MANs e WANs às Redes ATM,** Campus, 1995.

BLOOMBERG, **B-Unit White Paper**, enviado por e-mail em setembro de 2008, disponível em <thiago@mello.eng.br>, 2004.

PRIVARIS, **PlusID Datasheet**, Disponível em http://www.privaris.com/pdf/plusID_datasheet.pdf, acesso em 5 de outubro de 2008, 2007.

TRI-D, **Tri-D All Access Datasheet**, Disponível em http://www.tri-dsystems.com/docs-online/trid-d-all-access.pdf, acesso em 6 de outubro de 2008, 2008.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, **Guideline for Use of Advanced Authentication Technology Alternatives,** Disponível em http://www.itl.nist.gov/fipspubs/fip190.htm, acesso em 6 de outubro de 2008, FIPS, 1994.

ANEXO A

LEVANTAMENTO DE INFORMAÇÕES

Perguntas destinadas a ambos os grupos

I. Perfil do entrevistado

- Em qual empresa você trabalha?
- Qual a sua ocupação profissional?
- Há quanto tempo trabalha nesta empresa?
- Há quanto tempo trabalha nesta mesma ocupação dentro desta empresa?
- Qual a sua formação acadêmica?
- Em linhas gerais, qual a sua experiência profissional em outras empresas?

II. Contextualização da segurança da informação

- O que você entende por segurança da informação?
- Como a segurança da informação é vista pela empresa em que trabalha?

Perguntas destinadas ao grupo gerencial

III. Análise do B-Unit

- Qual a visão de negócio definida para o B-Unit?
- Como este dispositivo pode ser qualificado com relação à segurança da informação?
- Qual o tipo de mercado para o qual esta solução foi idealizada?
- Como era a autenticação do usuário remoto antes do B-Unit?
- Como é aceitação do B-unit pelo usuário final?
- Qual o grau de aceitação de outras soluções frente ao B-Unit? (?)
- Existe alguma chance do B-Unit ser comercializado para terceiros?
- O que poderia ser melhorado na solução de acesso remoto?
- Quais as melhorias propostas para o B-Unit em sua próxima versão?
- Há algum cronograma para que estas soluções entrem em vigor?

Perguntas destinadas ao grupo técnico

IV. Análise do B-Unit

- Tecnicamente, como é o funcionamento do B-Unit?
- Quais são os pontos fortes e fracos do B-Unit?
- Quais são os problemas mais comuns?
- Como é sua implantação? Erros e facilidades.
- O que poderia ser melhorado na solução de acesso remoto?
- Quais as melhorias propostas para o B-Unit em sua próxima versão?
- Onde o B-Unit não pode ser utilizado?

Perguntas destinadas ao usuário final

V. Análise do B-Unit

- Como era o acesso ao Bloomberg Anywhere antes do B-Unit?
- A mudança para o B-Unit causou algum desconforto? Quais?
- Quanto tempo levou para você se adaptar a nova tecnologia?
- Levando em consideração sua percepção de segurança, como você vê o papel do B-Unit nesse cenário?
- Você voltaria a utilizar a forma antiga de acesso ao Bloomberg Anywhere?
- O que poderia ser melhorado na solução de acesso remoto?
- Como a existência do B-Unit influencia na escolha deste provedor de serviços de informações em detrimento de outros (Broadcast, Reuters, etc..)?